

Exhibit D

From: Ward, Alec (CRT)
Sent: Monday, March 24, 2025 10:56 PM
To: donnie_fletcher@[REDACTED]
Subject: March 25 SWA Hearing
Attachments: 20205.3.24 - Revised CUAD Instagram Search Warrant_to JGK Chambers.pdf;
2017-10-22 DAG Memo - Protective Orders.pdf; 05.27.22 DAG Memo - Supplemental
Policy 2705b.pdf

Dear Mr. Fletcher,

In advance of tomorrow's 2:00 PM hearing *in the matter of a Search Warrant for Instagram account CUApentheiddinvest*, please find attached an amended Application for Search Warrant and Affidavit in Support. This is identical to the Application attached to the government's Letter of March 20, 2024 except insofar as the proposed Warrant includes language discussing the return of the warrant, per the judge's request of this afternoon.

We will also need to raise two additional issues with the Court. First, in the process of addressing the Court's question regarding the lack of a sworn affidavit, we discovered that this matter is in a different procedural posture than we originally believed, and we will accordingly need to modify the request articulated in our letter of March 20. Second, following additional internal consultation and research, the government believes that its request for a one-year period of precluded subscriber notice is consistent with the provisions of 18 U.S.C. § 2705(b). The attached publicly-available Department of Justice policy memoranda (also available online [here](#) and [here](#)) discuss the statutory authority for notice preclusion orders of up to and beyond one year and establish a Department-wide presumption against requesting § 2705(b) orders of more than one year in duration.

The government will be prepared to discuss both issues at the hearing.

Very respectfully,

Alec C. Ward

Trial Attorney | Criminal Section | Civil Rights Division
U.S. Department of Justice
Tel. [REDACTED] | [REDACTED]

Attachment 1



Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

May 27, 2022

MEMORANDUM FOR HEADS OF DEPARTMENT LAW ENFORCEMENT COMPONENTS
DEPARTMENT LITIGATING COMPONENTS
DIRECTOR, EXECUTIVE OFFICE FOR U.S. ATTORNEYS
ALL UNITED STATES ATTORNEYS

FROM: THE DEPUTY ATTORNEY GENERAL *Lina M. Maceo*

SUBJECT: Supplemental Policy Regarding Applications for Protective Orders
Pursuant to 18 U.S.C. § 2705(b)

This Memorandum provides clarification and direction for Department attorneys regarding protective orders pursuant to 18 U.S.C. § 2705(b) of the Stored Communications Act (SCA).¹ It supplements and clarifies the *Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b)*, issued by Deputy Attorney General Rod J. Rosenstein on October 19, 2017 (hereinafter the *2017 Policy*). New policy or procedures that appear within this Memorandum apply prospectively to all applications seeking Section 2705(b) orders filed on or after 30 days from the date this Memorandum is issued (including an application seeking to extend the period of an existing protective order). Updates to Justice Manual Section 9-13.700 consistent with this Memorandum will be forthcoming.

The SCA authorizes the government to access records maintained by providers of electronic communication service and remote computing services. In the modern era, these provisions provide a critical means for evidence collection and are a common tool in all types of federal criminal investigations. At the same time, the “SCA contains no default sealing or nondisclosure provisions” that would prohibit the subscriber from receiving notice from the provider about the government action. *In re Leopold to Unseal Certain Elec. Surveillance Applications & Ords.*, 964 F.3d 1121, 1129 (D.C. Cir. 2020) (internal quotation marks omitted).

¹ This Memorandum is intended only to assist in the management of the Department of Justice and the execution of its responsibilities. It is not intended to and does not create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding. This Memorandum does not impact or alter existing procedures governing protective orders pursuant to any other authority, including 18 U.S.C. § 2709(c) or the Termination Procedures for National Security Letter Nondisclosure Requirement, Federal Bureau of Investigation (Nov. 24, 2015).

Subject: Supplemental Policy Regarding Applications for Protective Orders
Pursuant to 18 U.S.C. § 2705(b)

Instead, Section 2705(b) permits the government to seek a court order that temporarily precludes a service provider from notifying another person of the existence of a warrant, subpoena, or court order issued pursuant to the SCA. To obtain such an order, however, the government must establish that there is reason to believe that notification of the existence of the warrant, subpoena, or court order “will”² result in (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of a potential witness; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

As noted in the *2017 Policy*, a protective order should be sought only after a prosecutor engages in a case- and fact-specific analysis. For example, protective orders may not be warranted when prosecutors take actions unlikely to alert targets of the investigation. Likewise, as investigations progress or become public, prosecutors should carefully consider whether such orders remain warranted, and, if so, for how long. Prosecutors should not assume that a prior need for a protective order means a subsequent order is necessary. While in many cases, particularly at an early stage of an investigation, one or more of these provisions may apply, case or other developments may reduce the likelihood of adverse results.

A prosecutor must provide a court with sufficient facts to permit the court to conduct the same case- and fact-specific analysis. In particular, as the *2017 Policy* stated, prosecutors applying for a § 2705(b) order must tailor the application to include the available facts that permit “an individualized and meaningful assessment regarding the need for protection from disclosure.” Applications should identify which of the pertinent factors apply and explain why.

Additional Section 2705(b) Orders After an Initial Order of One Year

The *2017 Policy* directs that prosecutors filing § 2705(b) applications may only seek to delay notice for one year or less, barring exceptional circumstances. Prosecutors may seek a second or additional protective order of equal or shorter duration if factors justifying non-disclosure continue to exist at the expiration of the original order, but requests should be supported with such additional, specific facts as may have been developed through the investigation.

To ensure that all facts and circumstances continue to be considered before applying for a protective order, applications for protective orders must be approved in writing by a supervisor whenever (a) it appears reasonably likely that the target(s) of the investigation already knows of the investigation’s existence or (b) the application is for a second or successive period of non-

² In contrast, a different subsection of 18 U.S.C. § 2705 dealing with the government’s more limited notice requirements permits a shorter, 90-day protective order where there is reason to believe that notification “may” have one of the enumerated adverse results. See 18 U.S.C. § 2705(a).

disclosure, such that the total period of the protective order exceeds 18 months.³ In order to maintain records of appropriate approvals, where approval is required, the litigating component making the application should maintain a record of such approval.

All sections and offices must establish a protocol by which they routinely review the need for § 2705(b) orders in an ongoing investigation or case. Such review can be accomplished through an office's regular case review.

The Department recognizes that judges may direct shorter or longer periods for orders, consistent with the language of § 2705(b), and this guidance does not affect those circumstances.

Closed Investigations and Termination of Section 2705(b) Orders

When closing an investigation or matter, a prosecutor must immediately assess whether there is a basis to maintain any outstanding protective orders issued pursuant to § 2705(b). If the prosecutor concludes that there is no such basis, the office must terminate the protective order and ensure the service provider is notified of any such termination (and, if necessary, notifying and/or seeking approval from the appropriate court before doing so). If the prosecutor believes there is a compelling reason to maintain a protective order, the prosecutor must seek approval from a supervisor to allow the protective order to remain in effect. Early termination of protective orders is not required for accounts that prosecutors believe were solely used as part of criminal infrastructure (e.g., accounts exclusively used to send malware to victims).

All sections and offices must establish a protocol by which an investigation's or case's outstanding § 2705(b) orders are reviewed as part of a case closing procedure.

Exceptional Circumstances and Section 2705(b) Protective Orders

Where there are "exceptional circumstances," the *2017 Policy* permits prosecutors to apply for initial or successive protective orders greater than one year in length. In almost all cases, these exceptional circumstances involve certain national security investigations with a significant foreign nexus, where the investigation differs in significant ways from a traditional criminal investigation.

To assist the Department in monitoring the use of this exception, prosecutors must notify the Department's Criminal Division (CRM) or National Security Division (NSD) when they seek

³ Supervisory approval for a successive protective order is not necessary if one or more target(s) of the investigation remains outside the United States and/or is a current fugitive.

Memorandum from the Deputy Attorney General

Page 4

Subject: Supplemental Policy Regarding Applications for Protective Orders

Pursuant to 18 U.S.C. § 2705(b)

a Section 2705(b) protective order of greater than one year due to “exceptional circumstances.”⁴ To ensure that the exception continues to be used only where warranted, for orders issued under “exceptional circumstances” for a period of greater than one year, supervisors in the section or office seeking such orders should conduct a review at least annually of such orders in order to confirm that any such unexpired orders remain necessary and notify CRM or NSD, as warranted, of the result of the review.⁵ The review should include an assessment of whether there remains a need for those protective orders.

Other Existing Department Requirements

All additional existing approval requirements related to the issuance of legal process—such as those governing sensitive investigative matters or legal process involving members of the news media—remains in effect.

Thank you for all you to do to serve the public and your dedication to the rule of law.

⁴ For all investigations and cases that otherwise have a Justice Manual notification, consultation, and/or approval requirement to NSD (or one of its Sections), notification of an application for a 2705(b) order should be made to the relevant NSD Section. For all other 2705(b) order applications, notifications should be made to CRM.

⁵ If a prosecutor believes a matter that is not a national security investigation with a significant foreign nexus still constitutes exceptional circumstances for purposes of this memorandum, he or she should consult with CRM and NSD before seeking a protective order for greater than one year. Consultation can simultaneously be done for a set of related matters that have a common reason for falling within this exception.

Attachment 2



U.S. Department of Justice

Office of the Deputy Attorney General

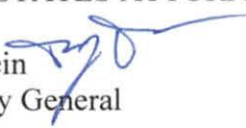
The Deputy Attorney General

Washington, D.C. 20530

October 19, 2017

MEMORANDUM FOR HEADS OF DEPARTMENT LAW ENFORCEMENT COMPONENTS
DEPARTMENT LITIGATING COMPONENTS
THE DIRECTOR, EXECUTIVE OFFICE FOR U.S. ATTORNEYS
ALL UNITED STATES ATTORNEYS

FROM:

Rod J. Rosenstein 
Deputy Attorney General

SUBJECT:

Policy Regarding Applications for Protective Orders
Pursuant to 18 U.S.C. § 2705(b)

This memorandum provides guidance and direction for Department of Justice attorneys and agents seeking protective orders pursuant to 18 U.S.C. § 2705(b) of the Stored Communications Act (SCA).¹ This guidance applies prospectively to all applications seeking protective orders, including both new orders and renewals, filed on or after 30 days of the date this memorandum is issued.

The SCA permits the government to obtain certain records and information from providers of electronic communications services or remote computing services relating to their customers or subscribers. Under the SCA, the government may compel the disclosure of different categories of information via subpoena, a court order under 18 U.S.C. § 2703(d), or a search warrant. The SCA does not by default forbid a provider from notifying anyone. Providers will be prohibited from voluntarily notifying their users of the receipt of legal process under the SCA only if the government obtains a protective order under 18 U.S.C. § 2705(b), based on a need for protection from disclosure.

Each § 2705(b) order should have an appropriate factual basis and each order should extend only as long as necessary to satisfy the government's interest. Prosecutors who are applying for § 2705(b) orders must follow the steps outlined below:

¹ This guidance is intended only to improve the internal management of the Department of Justice. It is not intended to and does not create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding. This memorandum does not impact or alter existing procedures governing protective orders pursuant to any other authority, including 18 U.S.C. § 2709(c) or the Termination Procedures for National Security Letter Nondisclosure Requirement, Federal Bureau of Investigation (Nov. 24, 2015).

1. Prosecutors must conduct an individualized and meaningful assessment regarding the need for protection from disclosure prior to seeking a § 2705(b) order and only seek an order when circumstances require.
2. In applying for a § 2705(b) order, prosecutors should tailor the application to include the available facts of the specific case and/or concerns attendant to the particular type of investigation. The prosecutor should identify which of the factors set forth in § 2705(b)(1)–(5) apply and explain why. For example, prosecutors might choose to include information about the relationship of the data sought to the subject(s) of the investigation or describe the potential for related accounts or data to be destroyed or otherwise made inaccessible to investigators. Similarly, prosecutors may identify concerns attendant to the risk of flight or harm to public safety in that particular investigation, including those concerns based on experience with similar types of investigations. The factors justifying protection from disclosure may be similar in many cases, particularly at the outset of an investigation. As appropriate, prosecutors may state the extent to which the stage of the investigation limits the availability of specific facts justifying the § 2705(b) order.²
3. Prosecutors may seek a single protective order that covers multiple grand jury subpoenas issued as part of the same investigation, or a single protective order that covers other sets of nearly-identical legal process in a discrete investigation. A single protective order for multiple items of process should be sought only if the facts justifying protection from disclosure are the same for all items of process covered by the order. Prosecutors should ensure that a copy of the protective order is served with each item of process covered by the order.
4. Barring exceptional circumstances, prosecutors filing § 2705(b) applications may only seek to delay notice for one year or less.³

² When applying for a § 2705(b) order to accompany a subpoena seeking basic subscriber information in an ongoing investigation that is not public or known to the subject(s) of the investigation, stating the reasons for protection from disclosure under § 2705(b)—such as the risk that subject(s) will flee, destroy or tamper with evidence, change patterns of behavior, or notify confederates—usually will suffice. At a later stage of the investigation, for example, when a search warrant is being sought, the prosecutor should include more specific facts, as available, in support of the protective order.

³ There may be exceptional circumstances in which orders of longer duration are necessary, such as in certain national security investigations that materially differ from routine criminal investigations. Orders seeking to delay notice beyond the time limit listed above shall be sought only with the written concurrence of a supervisor designated by the United States Attorney or the appropriate Assistant Attorney General, based upon facts and concerns that support a longer delay (*e.g.*, the suspect is an overseas fugitive who may travel internationally at some future time, if not alerted to the investigation).

5. The Department recognizes that judges may direct shorter or longer periods for orders, consistent with the language of § 2705(b).
6. If factors justifying protection from disclosure continue to exist at the expiration of the original order, subsequent extensions of equal or less duration may be sought. Requests should be supported with such additional, specific facts as may have been developed through the investigation.

The guidance was developed with input from many Department components and will be added to the U.S. Attorney's Manual. Nothing in this guidance is intended to indicate or imply that any existing protective order(s) issued by any court may be improper. If you have questions relating to the interpretation or recommended implementation of this guidance, please contact the Computer Crime and Intellectual Property Section of the Criminal Division at 202-514-1026.

Attachment 3

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
INSTAGRAM ACCOUNT
@CUAPARTHEIDDIVEST THAT IS
STORED AT PREMISES CONTROLLED
BY META PLATFORMS, INC.

TO BE FILED UNDER SEAL
AGENT AFFIDAVIT

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT
FOR STORED ELECTRONIC COMMUNICATIONS

I, [REDACTED], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Instagram account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), an electronic communications service and/or remote computing service provider headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications) further described in Section II of Attachment A. Upon receipt of the information described in Section II of Attachment A, government-authorized persons will review that information to locate the items described in Section III of Attachment A.

2. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3. This affidavit is based on my personal knowledge, information from other law enforcement officials, and documents reviewed during this investigation. This affidavit contains information necessary to support this application. It is not intended to include every fact observed by me or known to U.S. law enforcement personnel conducting this investigation.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that a violation of 18 U.S.C. § 875(c) have been committed by unknown persons associated with the Instagram account @cuapartheidinvest (the “Target Account”). There is also probable cause to search the information described in Section I of Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Section II of Attachment A.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. I am investigating an alleged interstate transmission of threats to injure a person or persons.

8. On March 14, 2025, the Instagram account @cuapartheiddivest (the “Target Account”) posted an image of a building spattered with a bright red substance and marked in black spray paint with an inverted triangle and the words “FREE THEM ALL.” The caption accompanying the post read: “anonymous submission: the Columbia President’s mansion has been redecorated. The people will not stand for Columbia University’s shameless complicity in genocide! The University’s repression has only bred more resistance and Columbia has lit a flame it can’t control. Katrina Armstrong you will not be allowed peace as you sic NYPD officers and ICE agents on your own students for opposing the genocide of the Palestinian people. WALKOUT AT 12:30PM. COLUMBIA MAIN GATES (Broadway/116)” A screen capture image of the image and caption (“the post”) is included below as Figure 1.



9. From my review of open-source materials on the Columbia University website, I know that Katrina Armstrong is the interim President of Columbia University. I know that the Columbia President's Mansion is located at 60 Morningside Drive, New York, New York 10027, within the Southern District of New York. From reviewing open-source Google Street View geo-located imaging data related to that address, I believe that the structure depicted in the post is, in fact, the south-facing façade of that address.

10. Based on my training and experience, I know that an inverted triangle is a symbol that has been used by militants affiliated with the terrorist organization Hamas in the ongoing Israel-Hamas conflict to designate targets for attack. Since the October 7, 2023 Hamas attack on Israel, in which approximately 1200 people were killed and approximately 250 people were taken hostage, Hamas's military wing, the Izz Al-Din Al-Qassam Brigades ("al-Qassam Brigades"), has regularly published videos from the fighting in Gaza in which Israeli military

forces about to be attacked are marked with a moving inverted red triangle¹. The below screenshots are examples from Hamas propaganda showing use of the inverted triangle:



An inverted red triangle marking an Israeli tank as a target (Source: Echoroukonline.com, November 14, 2023)



The triangle marking an Israeli tank before it is hit (Source: T.me/Qassambrigades, February 26, 2024)

¹ www.memri.org/reports/inverted-red-triangle-symbol-identified-hamas (last viewed March 15, 2025)



Israeli soldiers marked by red triangles (Source: T.me/Qassambrigades, February 12, 2024)

11. I also know the inverted triangle is frequently used in pro-Hamas memes and graphics on social media. For example, the screenshot below from a February 21, 2024 post on X shows Abu Obaida, the spokesman for the al-Qassam Brigades, emerging from an inverted triangle:



12. I also know the inverted triangle has been used in demonstrations on campuses in the United States. The inverted triangle, as shown below, has been used on posters, and can also be made by individuals joining their fingers together to make the triangle symbol:



13. From my review of public postings on the Target Account, I know that the Target Account purports to be the official Instagram account of Columbia University Apartheid Divest (“CUAD”). From review of the Target Account and from review of open-source media reports, in particular a November 14, 2023 op-ed in the Columbia Spectator student newspaper authored under CUAD’s organizational byline, I know that CUAD is a student-run organization, that, in its own words, “work[s] toward achieving a liberated Palestine and the end of Israeli apartheid by urging Columbia to divest all economic and academic stakes in Israel.”

14. From my review of postings on the Target Account, I know that CUAD expressly endorses and advocates the use of violence in furtherance of its organizational objectives. Specifically, I have reviewed an October 8, 2024 post made by the Target Account which included the statements: “we support liberation by any means necessary, including armed resistance” and “in the face of violence from the oppressor equipped with the most lethal military force on the planet, where you’ve exhausted all peaceful means of resolution, violence is the only path forward.” From reviewing open-source media reporting, including an October 1, 2024 Columbia Spectator article, I know that the Target Account made these statements as part of an open letter, posted to the Target Account, in support of a Columbia student named Khymani James, who had been disciplined by Columbia University for stating, during an Instagram live stream, that “Zionists don’t deserve to live” and “Be grateful that I’m not just going out and murdering Zionists.” Images of the open letter posted on the Target Account, taken on March 15, 2025, are included below:

A Letter from CUAD Leadership to Khymani James and Our Comrades in Solidarity

Last spring, in the midst of the encampments, Columbia University Apartheid Divest (CUAD) posted a statement framed as an apology on behalf of Khymani James. It is of the utmost importance that we clear the record regarding this statement. The statement was written by several CUAD organizers, not Khymani, and does not represent Khymani or CUAD's values or political lines. However, all CUAD organizers were complicit in *not maintaining our political line, keeping the statement public on our instagram, and in neglecting the mental and physical safety of Khymani.*

In light of this, we, as CUAD organizers, want to apologize first and foremost to Khymani. We caused irrevocable harm to you by contributing to the ostracization you experienced from your fellow students, fellow organizers, the media, and the public. **The anti-blackness and queerphobia that Khymani experienced, and continues to experience, from neo-liberals, neo-liberal media, and fascists is disgusting.** By issuing a so-called "apology," CUAD exposed Khymani to even more hatred from white supremacist and queerphobic liberals and fascists, along with the neo-liberal media. We deliberately misrepresented your experiences and your words, and *we let you down by purposefully playing into the media and the public's neo-liberal co-optation of our encampments and our movement for Palestinian liberation.*

We also want to issue a public apology to all those fighting for Palestinian liberation that we alienated by **compromising our values and tailoring our actions and narrative to the mainstream media.** As an organization, we set our movement back. We alienated members of our community, utilizing the same tactics the state uses to isolate organizers working to push the boundaries of what is acceptable. Who keeps us safe? We keep us safe. But in recent months, we have failed Khymani and others in keeping them safe. And for that, we sincerely apologize and will continue working towards holding ourselves accountable by **keeping true to our political lines, learning in public, refusing to treat one another as disposable, and not bending to neo-liberal media.**

We support liberation by any means necessary, including armed resistance.

Part of our collective liberation includes recognizing that pandering to liberal media to make the movement for liberation palatable and digestible sets us back. *Everyday, neo-liberal media commits acts of violence against Palestinians by dehumanizing Palestinians as people who deserve to experience genocide, twisting narratives to frame Palestinian freedom fighters as terrorists, and neglecting to publicize the violent realities of Israeli apartheid and occupation.*



cuapartheiddivest • Follow



cuapartheiddivest A Letter from CUAD Leadership to Khymani James and Our Comrades in Solidarity. Please read thoroughly.

22w



robbykurnia3 Fuuuuucc. Around and find out

2d Reply



aninstush Eewww this is gross 🤢

2d Reply



sculptor.stefan.vladescu is shmuck schumer part of this very laughable idiotic movement, if yes then it's



Liked by leximcmnamenin and others
October 8, 2024

Log in to like or comment.



cuapartheiddivest • Follow



cuapartheiddivest A Letter from CUAD Leadership to Khymani James and Our Comrades in Solidarity. Please read thoroughly.

22w



robbykurnia3 Fuuuuucc. Around and find out

2d Reply



aninstush Eewww this is gross 🤢

2d Reply

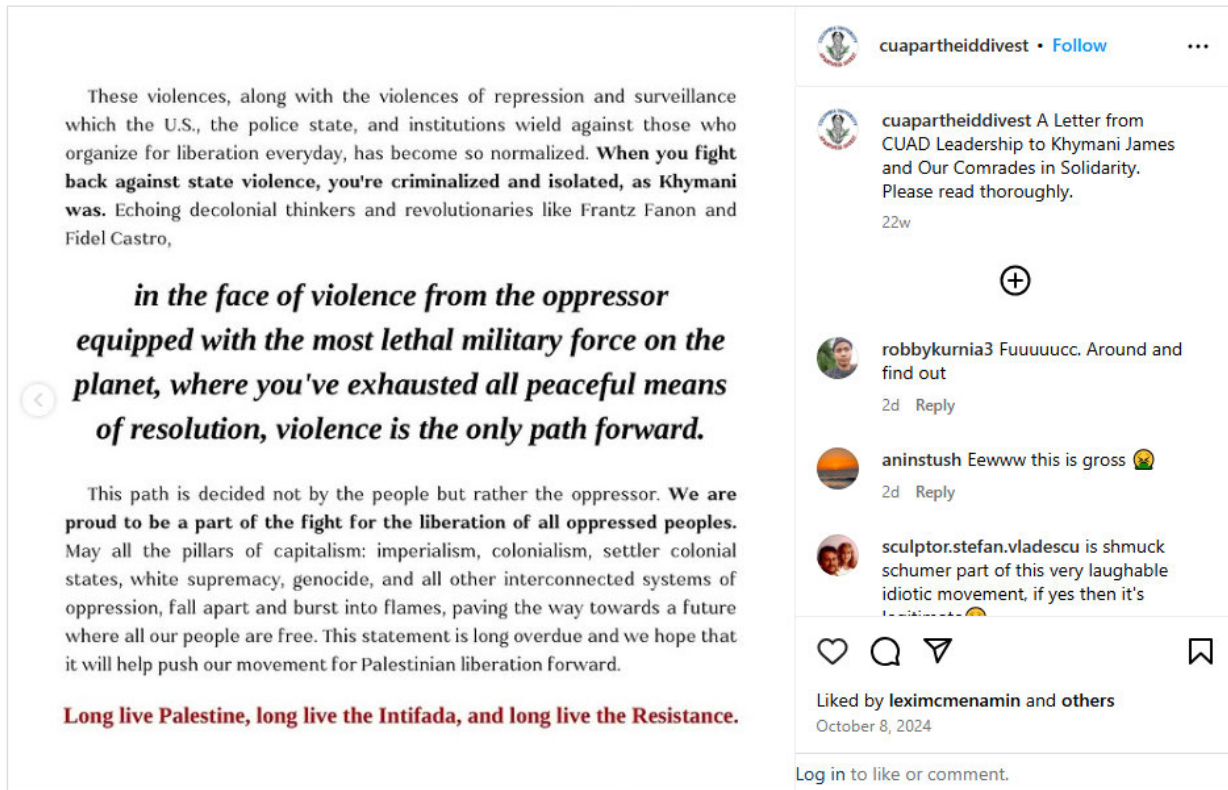


sculptor.stefan.vladescu is shmuck schumer part of this very laughable idiotic movement, if yes then it's

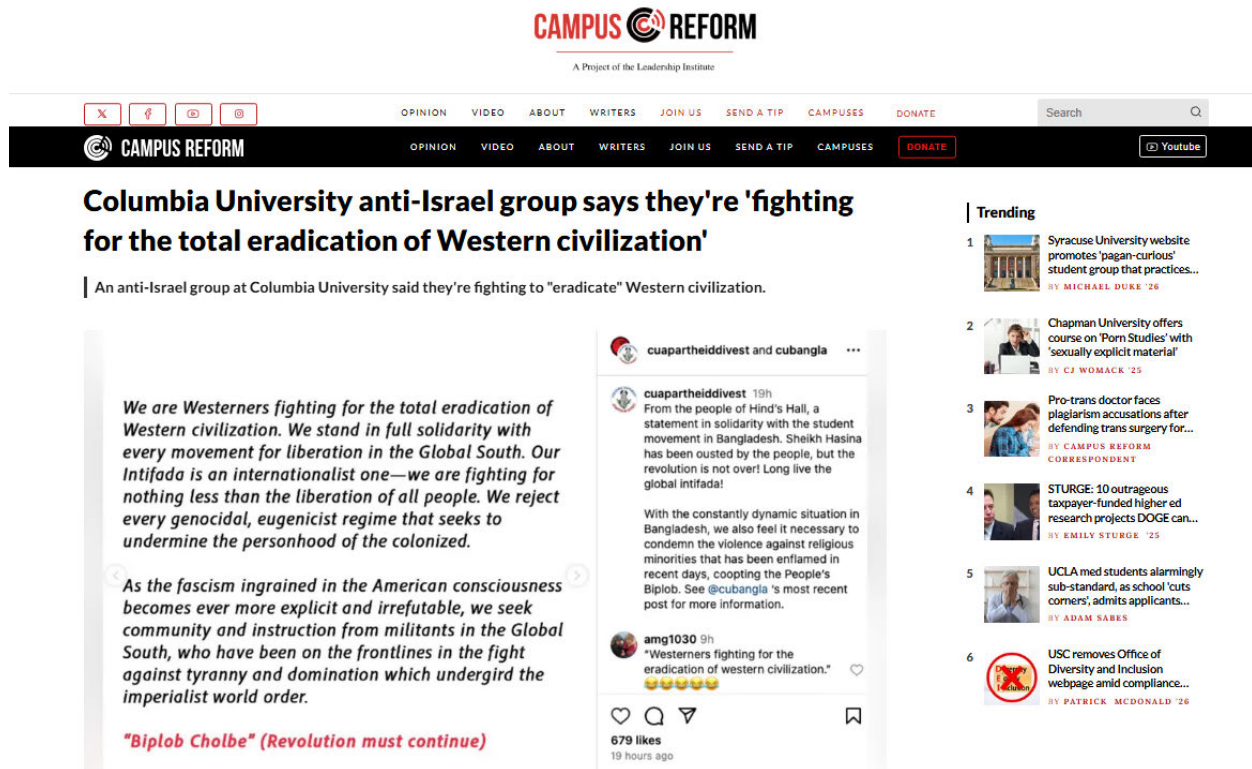


Liked by leximcmnamenin and others
October 8, 2024

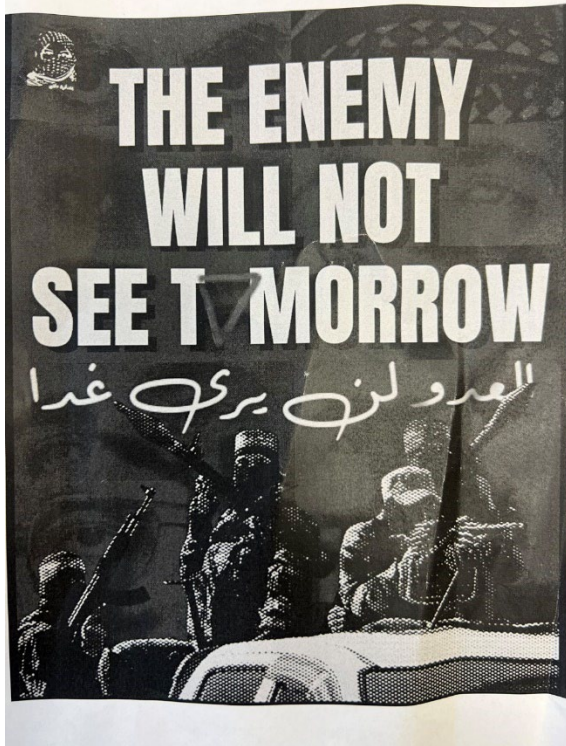
Log in to like or comment.



15. I have also reviewed open-source media reports that included photographs of an image posted to the Target Account that is no longer publicly-viewable and that stated, in the context of a broad expression of support for a student movement in Bangladesh, that CUAD “is fighting for the total eradication of Western civilization.” A screen-capture of the since-deleted post, as reported in an August 8, 2024 open-source news article on the website Campus Reform, is included below:



16. On January 21, 2025, four masked individuals entered a “History of Modern Israel” class at Columbia University. Refusing the professor’s requests to leave, the group handed out printed flyers while one member read a prepared statement, preventing the class from proceeding. According to open-source media reports and social media posts purporting to be authored by students present in the classroom at the time, one of the flyers that the group distributed consisted of a picture of three armed militants, wearing similar masks to those worn by the disruptors, and bearing the superimposed text “THE ENEMY WILL NOT SEE TOMORROW.” The first “O” in the word “TOMORROW” was replaced by an inverted triangle, as shown here:



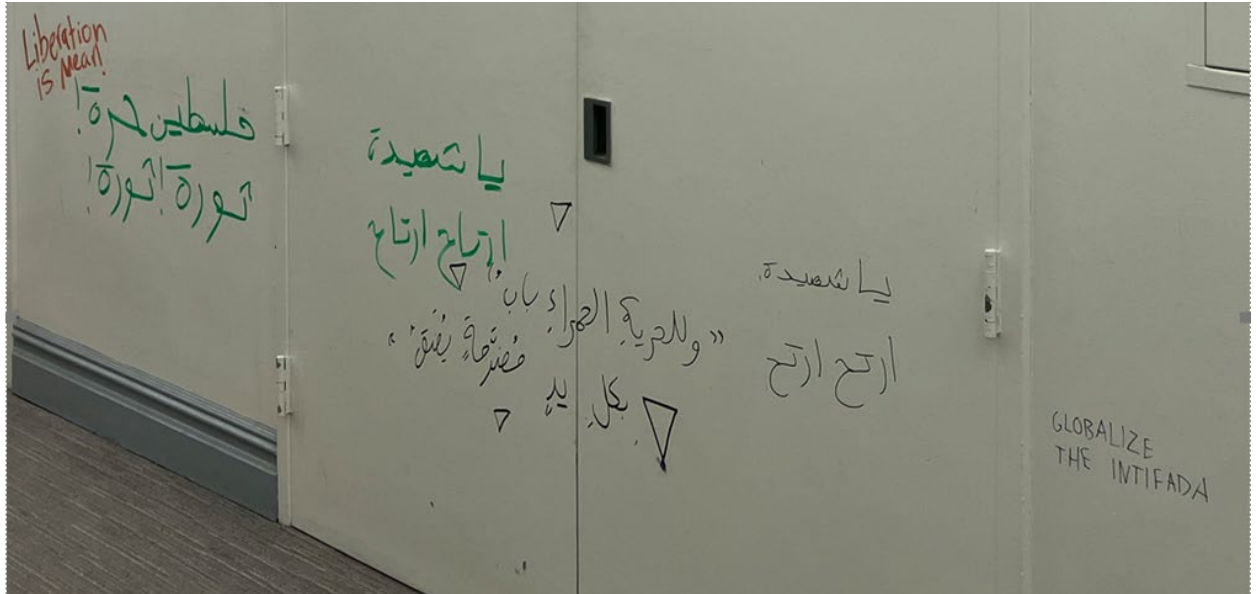
17. On February 23, 2025, Barnard University announced that it would expel two students for their role in the January 21 class disruption. On the same day, CUAD took credit for the Jan 21 disruption in an Instagram post on the Target Account. The post contains a video of the event that is approximately 30 seconds long and contains sub-titles that read “Israel is backed by the world’s most violent imperialist forces and they attempt to erase the truth from our collective consciousness. To make this occupation seem moral and okay. To make it seem like a world without Israel can’t exist but we know it can and has. Hopefully we got here in time to go over the syllabus and we can find out what modern Israel even is... There are Palestinian grandmothers who are older than the state itself.” A still shot of the video from the Target Account is shown here:



18. On February 26, 2025, a group of masked individuals forced entry into Milbank Hall, a building at Barnard that includes the Dean's office and other administrative offices. A Barnard security employee sustained minor injuries while trying to block the group's entry to the building. The group staged a sit-in in the hallway outside the Dean's Office and circulated a written list of demands that included the recission of the two students expelled in connection with the January 21 class disruption. A photograph of the group is shown here:



19. Before eventually leaving the building several hours after entering, unidentified members of the group vandalized the walls of the hallway they had been occupying. The graffiti included four upside-down triangles alongside Arabic script, as shown below:



20. A preliminary translation of the Arabic text shown indicates the following: The green ink to the left of the doors says “Free Palestine! Revolution! Revolution!” The green and black text written on the doors says “Oh martyr, relax/rest easy, relax/rest easy.” I know from training and experience that individuals who carry out suicide bombing attacks or who die while fighting on behalf of a terrorist organization, such as Hamas, are often praised by the terrorist organization as “martyrs.”

21. A preliminary translation of the black text on the door surrounded by the four inverted triangles says, "Freedom has a red door that is knocked on by every stained/bloodied hand". Of note, this is a line from a poem written by Ahmed Shawqi, an Egyptian poet, in 1926. In January 2025, Al Jazeera broadcast a video of Yahya Sinwar reciting the line. Sinwar was one of the senior Hamas leaders who orchestrated the October 7, 2023 attack on Israel, and was charged via complaint in the Southern District of New York with numerous terrorism offenses

resulting in death². In a September 3, 2024 press release, the Attorney General at the time said “The Justice Department has charged Yahya Sinwar and other senior leaders of Hamas for financing, directing, and overseeing a decades-long campaign to murder American citizens and endanger the national security of the United States³.” Sinwar was killed in Gaza in October 2024.

22. The photo above also shows the phrase “GLOBALIZE THE INTIFADA” in English. I know from training and experience “intifada” refers to Hamas’s decades-long campaign of violence against Israel that has resulted in death and injury to hundreds of people. The phrase “GLOBALIZE THE INTIFADA” appears to be a call to use the same violence employed by Hamas in other regions of the world, including the United States. As noted above in paragraph 14, the October 8, 2024 post to the Target Account includes the phrase “long live the intifada.”

23. The Target Account claimed credit for the February 26 event on behalf of CUAD on February 27.

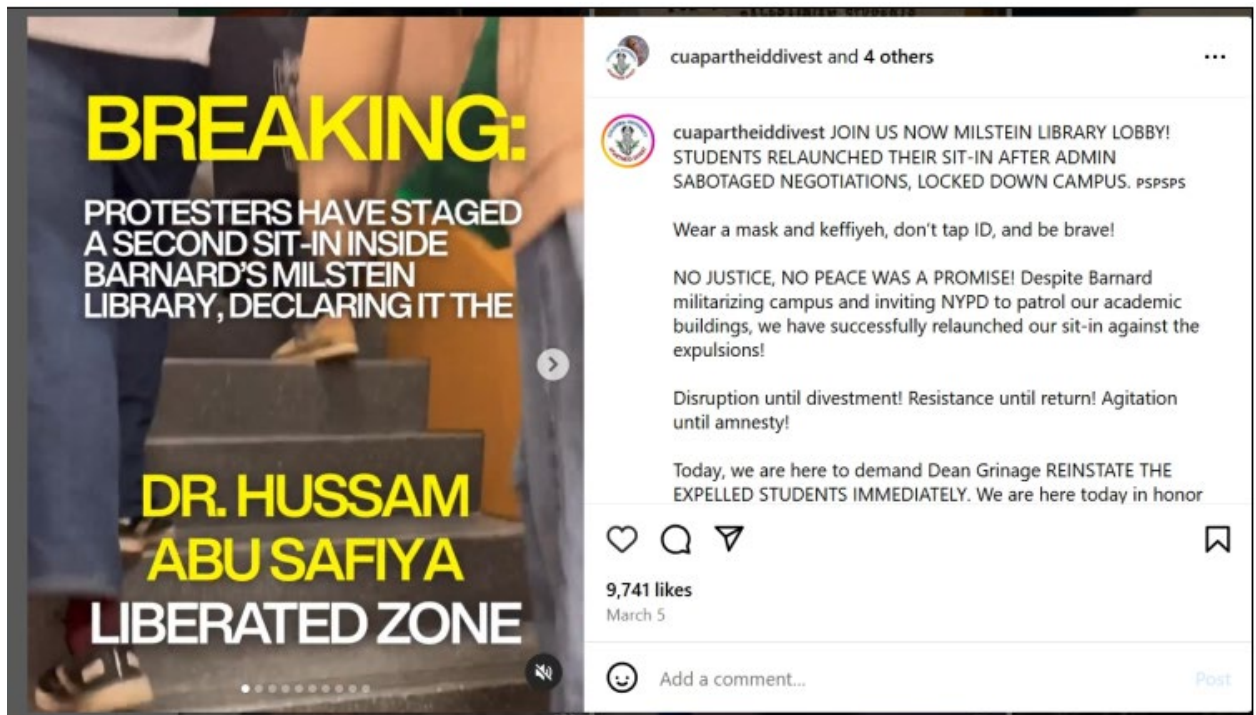
24. On March 5, 2025, a group of masked individuals forced entry into the lobby of the Milstein Center, a multi-use building at Barnard which includes the main college library. The group obstructed normal usage of the building facilities and refused administrators’ directions to leave. Another security guard sustained minor injuries during the event. While inside, members of the group distributed more leaflets, one of which purported to be authored by the “Hamas Media Service” and to offer Hamas’ justification for the October 7 terror attacks. Most of the

² ECF No. 2 1:24-mj-00438 (SDNY Feb 1, 2024)

³ www.justice.gov/archives/opa/pr/justice-department-announces-terrorism-charges-against-senior-leaders-hamas

group left the building as SRG officers entered, and then reformed in the outdoor courtyard outside the lobby. NYPD-SRG attempted to disperse this re-formed group, and a number of physical confrontations between group members and SRG officers ensued, resulting in the arrest of nine individuals.

25. The Target Account took credit for the March 5 occupation in a post the same day, as shown here:



26. Based on these facts, I submit that there is probable cause to believe that the Target Account's March 14, 2025, transmission of the above-described photograph and caption constitutes interstate communication of a threat to injure, in violation of 18 U.S.C. § 875(c). The Target Account purports to speak on behalf of a group that has expressly endorsed the use of violence for the accomplishment of its stated goals. The post includes the inverted triangle

symbol, which is used by Hamas to designate structures and individuals as targets for violent attack. In the post, the inverted triangle is displayed alongside a bright red substance applied to the official residence of the Columbia president, who is designated by name in the post and whom the post warns “will not be allowed peace.”

BACKGROUND CONCERNING INSTAGRAM⁴

27. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510.

Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

28. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user’s full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

29. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol (“IP”) addresses used to create

⁴ The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: “Privacy Policy,” <https://privacycenter.instagram.com/policy/>; “Information for Law Enforcement,” <https://help.instagram.com/494561080557017>; and “Help Center,” <https://help.instagram.com>.

and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

30. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if “added” to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

31. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

32. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

33. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

34. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

35. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

36. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

37. An Instagram “story” is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator’s “Stories Archive” and remain on Meta’s servers unless manually deleted. The usernames of those who viewed a story are visible to the story’s creator until 48 hours after the story was posted.

38. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram’s long-form video app.

39. Instagram Direct, Instagram’s messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with “disappearing” photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can’t view their disappearing messages after they are sent but do have access to each message’s status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

40. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

41. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be “followed” to generate related updates from Instagram. Meta retains records of a user’s search history and followed hashtags.

42. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

43. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user’s identity and activities, and it can also reveal potential sources of additional evidence.

44. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

45. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone

numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

46. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. Specifically, the evidence may establish who authored and transmitted the posts containing the above-discussed threatening statements.

47. Specifically, the user’s account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

48. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a

plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

49. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

REQUEST FOR NON-DISCLOSURE AND SEALING

50. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. Some of the evidence in this investigation is stored electronically. If alerted to the existence of the warrant, the subjects under investigation could destroy that evidence, including information saved to their personal computers. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

51. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter,

and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

CONCLUSION

52. Based on the forgoing, I request that the Court issue the proposed search warrant.

53. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

[REDACTED]
Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission of this Affidavit by reliable electronic means,
pursuant to Federal Rules of Criminal Procedure 41(d)(3) and 4.1,
on _____, 2025

Honorable John G. Koeltl
United States District Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH
OF INFORMATION ASSOCIATED
WITH INSTAGRAM ACCOUNT
@CUAPARTHEIDDIVEST THAT IS
STORED AT PREMISES
CONTROLLED BY META
PLATFORMS, INC.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Meta Platforms, Inc. (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

1. Warrant. Upon an affidavit of [REDACTED] of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the Instagram account @cuapartheiddinvest, maintained at premises controlled by Meta Platforms Inc., contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 14 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence and/or flight from prosecution, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Return. Upon receipt of records from the provider, the Investigative Agency executing this warrant shall return this Warrant and an Inventory of any records seized pursuant thereto, to the Magistrate Judge then on criminal duty in the U.S. District Court for the Southern District of New York.

4. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Date Issued

Time Issued

UNITED STATES DISTRICT JUDGE

Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Meta Platforms, Inc. (the “Provider”), headquartered at 1 Meta Way, Menlo Park, CA 94025, and applies to all content and other information within the Provider’s possession, custody, or control associated with the Instagram account @cuapartheiddivest (active on, but not limited to, March 13, 2025) (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or other information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- A. All business records and subscriber information, in any form kept, pertaining to the account, including:
 - 1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
 - 2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts

- (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);
3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
 4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
 5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;
 6. Internet Protocol (“IP”) addresses used to create, login, and use the account, including associated dates, times, and port numbers, from January 1, 2024, to present;
 7. Privacy and account settings, including change history; and
 8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;
- B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from January 1, 2024, to present;
- C. All content, records, and other information relating to communications sent from or received by the account from January 1, 2024, to present, including but not limited to:
1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;
 2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
 3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;
- D. All content, records, and other information relating to all other interactions between the account and other Instagram users from January 1, 2024, to present, including but not limited to:
 1. Interactions by other Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;
 2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;
 3. All contacts and related sync information; and
 4. All associated logs and metadata;
- E. All records of searches performed by the account from January 1, 2024, to present; and
- F. All location information, including location history, login activity, information geotags, and related metadata from January 1, 2024, to present.

Meta is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

III. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 875(c) including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- A. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- B. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
- C. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.